1252.239-70 Security Requirements for Unclassified Information Technology Resources.

As prescribed in 1239.106-70, insert the following clause:

SECURITY REQUIREMENTS FOR UNCLASSIFIED INFORMATION TECHNOLOGY RESOURCES (DATE)

(a) The Contractor shall be responsible for information technology security for all systems connected to a Department of Transportation (DOT) network or operated by the Contractor for DOT, regardless of location. This clause is applicable to all or any part of the contract that includes information technology resources or services in which the Contractor has physical or electronic access to DOT information that directly supports the mission of DOT. The term "information technology," as used in this clause, means any equipment or interconnected system or subsystem of equipment, including telecommunications equipment, that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. This includes both major applications and general support systems as defined by OMB Circular A-130. Examples of tasks that require security provisions include—

(1) Hosting of DOT e-Government sites or other IT operations;

(2) Acquisition, transmission, or analysis of data owned by DOT with significant replacement cost should the contractor's copy be corrupted; and

(3) Access to DOT general support systems/major applications at a level beyond that granted the general public, *e.g.*, bypassing a firewall.

(b) The Contractor shall develop, provide, implement, and maintain an IT Security Plan. This plan shall describe the processes and procedures that the Contractor will follow to ensure appropriate security of IT resources developed, processed, or used under this contract. The plan

shall describe those parts of the contract to which this clause applies. The Contractor's IT Security Plan shall comply with applicable Federal Laws that include, but are not limited to, 40 U.S.C. 11331, the Federal Information Security Management Act (FISMA) of 2002, and the E-Government Act of 2002. The plan shall meet IT security requirements in accordance with Federal and DOT policies and procedures, as amended during the term of this contract, which include, but are not limited to the following:

(1) OMB Circular A-130, Managing Information as a Strategic Resource;

(2) National Institute of Standards and Technology (NIST) Guidelines;

(3) DOT CIO IT Policy (CIOP) compendium and associated guidelines;

(4) DOT Order 1630.2C, Personnel Security Management; and

(5) DOT Order 1351.37, Departmental Cyber Security Policy.

(c) Within 30 days after contract award, the contractor shall submit the IT Security Plan to the DOT Contracting Officer for review. This plan shall detail the approach contained in the offeror's proposal or sealed bid. Upon acceptance by the Contracting Officer, the Plan shall be incorporated into the contract by contract modification.

(d) Within six (6) months after contract award, the Contractor shall submit written proof of IT Security accreditation to the Contracting Officer. Such written proof may be furnished either by the Contractor or by a third party. Accreditation shall be in accordance with DOT policy available from the Contracting Officer upon request. The Contractor shall submit along with this accreditation a final security plan, risk assessment, security test and evaluation, and disaster recovery plan/continuity of operations plan. The accreditation and accompanying documents, to include a final security plan, risk assessment, security test and evaluation, and

disaster recovery/continuity of operations plan, upon acceptance by the Contracting Officer, will be incorporated into the contract by contract modification.

(e) On an annual basis, the Contractor shall verify in writing to the Contracting Officer that the IT Security Plan remains valid.

(f) The Contractor shall ensure that the official DOT banners are displayed on all DOT systems (both public and private) operated by the Contractor that contain Privacy Act information before allowing anyone access to the system. The DOT CIO will make official DOT banners available to the Contractor.

(g) The Contractor shall screen all personnel requiring privileged access or limited privileged access to systems operated by the Contractor for DOT or interconnected to a DOT network in accordance with DOT Order 1630.2C Personnel Security Management, as amended.

(h) The Contractor shall ensure that its employees performing services under this contract receive annual IT security training in accordance with OMB Circular A-130, FISMA, and NIST requirements, as amended, with a specific emphasis on rules of behavior.

(i) The Contractor shall provide the Government access to the Contractor's and subcontractors' facilities, installations, operations, documentation, databases and personnel used in performance of the contract. The Contractor shall provide access to enable a program of IT inspection (to include vulnerability testing), investigation, and audit (to safeguard against threats and hazards to the integrity, availability and confidentiality of DOT data or to the function of information technology systems operated on behalf of DOT), and to preserve evidence of computer crime.

(j) The Contractor shall incorporate and flow down the substance of this clause to all subcontracts that meet the conditions in paragraph (a) of this clause.

(k) The Contractor shall immediately notify the Contracting Officer when an employee who has access to DOT information systems or data terminates employment.

(End of clause)